Ricoh Security Solutions

GDPR from the Information Security Perspective **Q&A**

RICOH
imagine. change.

Ricoh's Security Webinar ***GDPR from the Information Security Perspective*** raised some great questions from attendees on what GDPR really means, its implications for businesses of all sizes, and what businesses can do now to prepare for compliance.

Here are the answers to those questions from our security experts and webinar hosts, Mike Irvine and Max Metzger.

Mike Irvine
Ricoh Europe

Mike is Vice President & General Manager, Software & European Programme Management at Ricoh Europe. With over 35 years' experience in IT and business solutions, Mike is Ricoh's resident expert in business security.

Max Metzger
Freelance Reporter & Copywriter

Max is a freelance journalist and writer covering technology. After a two year stint at SC Magazine UK as a reporter, he went freelance and has since been involved in a variety of print and broadcast projects in and out of the cyber-security industry.

*The questions in this document were asked by attendees of Ricoh's Webinar and Q&A entitled 'GDPR from the Information Security Perspective', delivered in February 2018. The answers provided are based on the personal experience, research and expertise of our webinar hosts and should be taken by businesses as guiding information only. To book a security consultancy with your local Ricoh representative, visit us at ricoh-europe.com/contact-us For further information refer to the Information Commissioner's Office Guide to GDPR at ico.org.uk

Q In terms of GDPR gap analysis what sorts of questions do you think should be asked?

A Ricoh Europe response:

MI The first step is to identify what personal information you hold and why you are holding it. You will need this information to complete your Article 30 Record. This is a written record of what personal data is held, on what legal basis, for what purpose and how it is processed. This is needed BEFORE processing takes place.

Once you have identified what personal information you have a justifiable need for, you will then need to assess how you can ensure its privacy. You should also ensure that you are not holding personal information for which you have no need.

Q GDPR is about customer data as well as our own employee data, right?

A Ricoh Europe response:

MI Yes. GDPR applies to any information relating to an identified or identifiable natural person. It makes no distinction about the relationship with that person.

MM It's about any data you hold which could be personally identifiable. That could be absolutely anyone whose data you hold. So yes, customer data, employee data and the data of anyone else that you hold.

Q What constitutes 'personal' information?

A Ricoh Europe response:

MI This is any information relating to an identified or identifiable natural person. GDPR extends the current definition to include information such as location data and online identifiers or "cookies".

MM This is anything that could be tied to the subject of that data (i.e. the person whose data it is). Names, addresses and dates of birth are clear examples of personal data, but this can also extend to financial information, healthcare records and authoritative identity documents such as passports.

Q What if my data is in the cloud and the cloud is compromised, and data is breached. Who gets the penalty? Me or the cloud provider?

A Ricoh Europe response:

MI Both the data processor and data controller could be held liable, depending on who is responsible for the breach.

Data controllers have vast obligations under GDPR.

Under the GDPR, data subjects can also bring claims directly against data processors.

The data processor would be liable if they have: (i) not complied with directly applicable obligations for data processors under the GDPR; or (ii) departed from the instructions of the data controller and acted on its own decisions.

MM GDPR requires you to take responsibility for the security of your third parties - so you'd need to assess whether they too are GDPR compliant.

Q Does Personally Identifiable Information (PII) in GDPR apply to former employees as well as customers?

A Ricoh Europe response:

MI Yes. GDPR applies to any information relating to an identified or identifiable natural person. It makes no distinction about the relationship with that person.

Q How do I prove to a customer that I have deleted the data they requested me to delete?

A Ricoh Europe response:

MI

It is important to firstly identify what data is held, why it is held, and how it is held. You then must implement processes for managing the data, including deletion. Being able to share robust processes and give written assurances of deletion will normally satisfy most data subjects.

Q Do you think a Data Loss Prevention (DLP) system is a must in order to make sure the policies are being followed?

A Ricoh Europe response:

MI

DLP is a very important tool and provides good functionality. However, before identifying which tools are required it is important to conduct a privacy and security risk assessment. Just like any security tool, DLP should be implemented to address a specific need or risk.

Q According to GDPR do I need to have logs for the read access to the system?

A Ricoh Europe response:

MI

Retaining logs for who has accessed data and amended data is very useful. These logs can help an organisation to govern their information security and to prove adequate controls are in place.

Logs should be used as part of a security solution in response to the identified risks, and to enable businesses to provide accurate reports if required to do so in accordance with GDPR.

Q Are there any guidelines available for what rules apply to different size companies e.g. with less than £1m annual revenue, £1m-10m, £10m-50m, £50m or greater?

A Ricoh Europe response:

MI

GDPR applies to all organisations irrespective of size. The primary focus of the regulation is to improve the privacy of EU data subjects.

For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities. The UK Information Commissioner has published useful guidelines aimed at small organisations: https://ico.org.uk/for-organisations/business/. Organisations should seek advice from their local authorities.

MM

GDPR rules apply for companies big and small, as do the fines.

There are, however, some things that are worth considering for smaller companies. Your Data Protection Officer (DPO), for example, does not have to be a new hire, but can be somebody who already works in your organisation, whose current responsibilities align with that of the DPO. A third party service can also fulfil the role.

Q As an example of practical impact: Would it be fair and lawful to store personal customer data in log files for debugging purposes (e.g. social security number of a customer's job applicant in document title), and what would be the appropriate security measures?

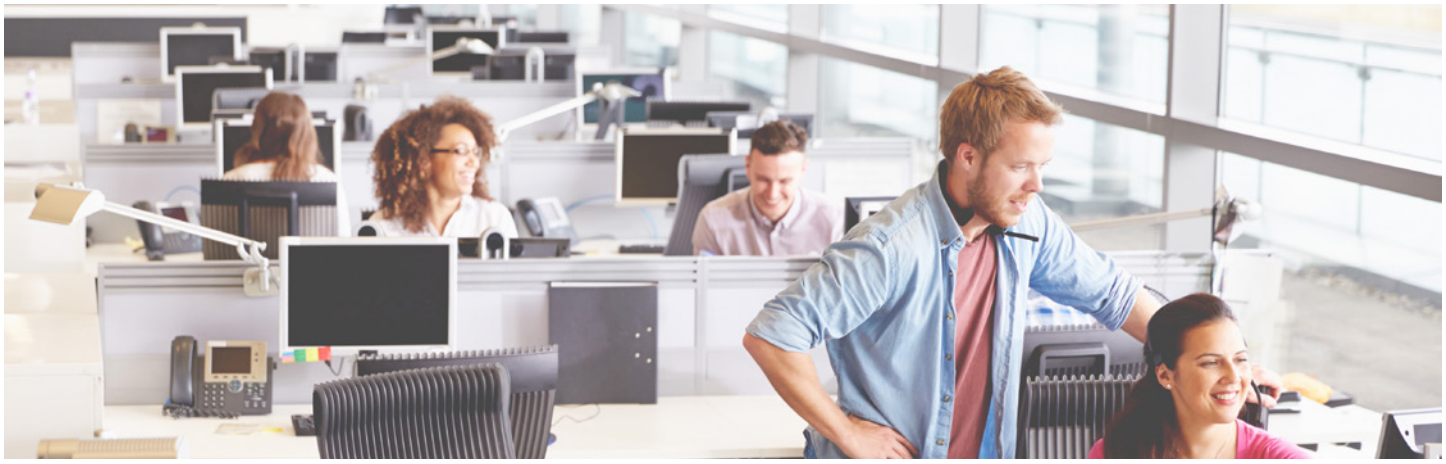
A Ricoh Europe response:

MI

A Data Controller can hold and store personal information that is needed to perform their business activity. They must identify and register what data they hold and for what purpose. They then must provide adequate security in order to ensure the confidentiality, integrity and availability of that data.

Keeping personal data in log files may not be unlawful but it does present an increased risk. How will the Data Controller know and declare the personal data is in the log files? How can they ensure that it is deleted when no longer required and how can they prevent misuse?

This risk extends to organisations providing their systems as a Data Processor. They must declare and manage all of the personal information that they hold.



Q In our company, we rely a lot on cold-calling, and of course we record all details of conversations, including contact details/responsible persons. How does GDPR apply to this?

A Ricoh Europe response:

MI

The primary principle of GDPR is "privacy by design". Individuals' rights include consent to marketing, Subject Access Requests (SARs) and the right to be forgotten. SARs will be free of charge and carried out in one month (rather than 40 days).

Consent by individuals must be given proactively (i.e. no more pre-ticked boxes) and can be easily withdrawn. Increased publicity means individuals are likely to be more aware of their rights, and therefore more likely to exercise them. This is likely to have a significant impact on cold calling organisations. I recommend seeking advice from a legal specialist.

The Information Commissioner's Office (ICO) has published this guidance on their website: "You must not make marketing calls to any number listed on the Telephone Preference Service (TPS) or Corporate TPS (CTPS), unless that person has specifically consented to your calls. You can call a number if it is not listed on the TPS or CTPS. So you need to screen call lists against the TPS and CTPS. You must allow your number to be displayed."

Q If an individual was to make a complaint based on a breach of GDPR, how would they do that?

A Ricoh Europe response:

MI

Data subjects will have the right to submit a SAR (Subject Access Request). SARs will be free of charge and must be carried out in one month (rather than 40 days).

A Data Subject will be able to register concerns about a Data Controller and / or Data Processor to the national authorities. The actual process and name of the organisation will vary country to country.

MM

I think they would take their complaint directly to the local regulator. In the case of the UK that would be the ICO, which already has processes in place to handle complaints based on previously existing data protection law. A complaint can also be pursued through national courts.

Q What are the anticipated short-term actions by data protection agencies across the EU during 2018?

A Ricoh Europe response:

MI This will vary by country. All will be preparing by taking steps they see necessary to govern the new regulations. Some countries are known to be recruiting additional staff and conducting training in preparation.

It is currently enough to register with the local regulator and provide basic information about the data you hold. Under GDPR the regulator can visit at any time. You must be ready to provide records to prove your compliance.

MM If you look at ICO enforcement activity it has been increasingly willing to hand out fines over the last few years. Under Elizabeth Denham, current Information Commissioner and an avowed fan of the GDPR, the ICO has handed out some of the largest fines in its history. This, some have said, is in direct preparation for the advent of GDPR in May.

Q Many industry sales people are saying that 'their' photocopiers/ Multi Function Printers (MFPs) can make companies GDPR compliant. How would you respond to this?

A Ricoh Europe response:

MI This is not correct. Security features on MFPs and supporting software can help to improve privacy and security which will contribute towards compliance. These include features such as disk overwrite security, user authentication, encryption, and secure document printing. However, if adequate security is not also implemented on PCs, servers and networks the risk of data breach and non-compliance will remain.

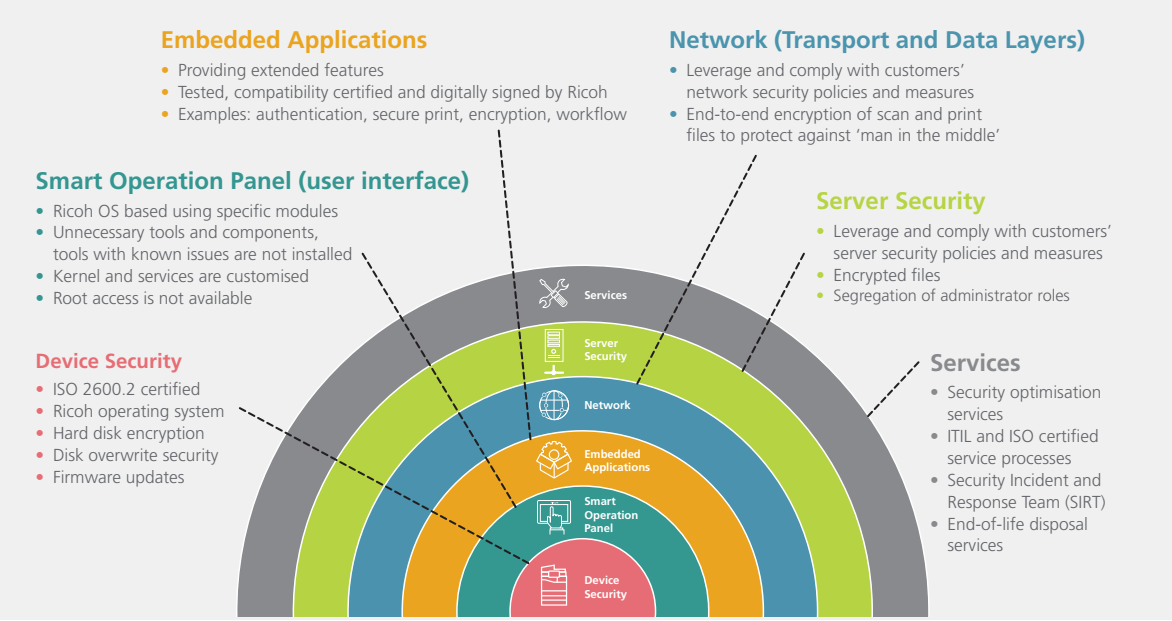
There are also vendors of security tools and IT systems making the same claim. The fact is that there is no "out of the box solution" for GDPR compliance.

Q Can you confirm what is meant by 'Trusted Platform Components'?

A Ricoh Europe response:

MI The standard industry definition is: "A Trusted Platform is a computing platform that has a trusted component". Ricoh uses this term to define our layered approach to security which comprises of hardware, software and services.

This layered approach is illustrated & explained below:



The device - At the heart of any Ricoh model we have the device. These are designed, manufactured and implemented with security as a core requirement. The Ricoh-only operating system does not share vulnerabilities that are present in many commercial off-the-shelf operating systems and our devices are certified to IEEE2600.2 as standard. Hard disk encryption and disk overwrite security ensure that data being processed remains confidential.

The Smart Operation Panel (SOP) provides the user interface - In a similar manner to the MFP, the SOP uses a Ricoh-only operating system. No unnecessary components are installed and root access is not available. Ricoh has worked hard to ensure that device security is not weakened by the introduction of the SOP.

Smart applications - These can be embedded on the SOP providing additional functionality to the user, including workflow and data capture. Some applications provide essential security features. These include secure print capability, card access and encryption. Applications are developed by Ricoh or Ricoh Developer Programme members and all applications must pass Ricoh compatibility testing and be digitally signed before they can run on the SOP.

Network and servers - Irrespective of who manages the IT infrastructure, Ricoh ensures that our products and services comply with our customers' IT and network security policies. End-to-end encryption of print and scan files, encryption of data on servers and segregation of administrator duties are techniques used to protect against "man-in-the-middle" or "inside jobs".

Services - A comprehensive range of security services encompasses our entire offering. This includes consultancy and managed services to assist customers to monitor, optimise and manage their document and information security.

We also have a range of end-of-life services which will ensure that the Random-access Memory (RAM) and Hard Disk Drive (HDD) of retired customer devices are wiped clean before disposal.

Q When a contact wants to be “forgotten”, how does that work?

A Ricoh Europe response:

MI

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

Organisations must endeavour to comply with the request using their documented processes. They may need to be able to demonstrate this during audits.

Q All of the programmes we use to store client data are password protected. Is that enough to be counted as secure in terms of GDPR regulations?

A Ricoh Europe response:

MI

GDPR requires adequate security according to the risk. What risks have been identified? It is unlikely that password protection alone will be sufficient. Remember the CIA (Confidentiality, Integrity and Availability) requirement. A password will contribute to confidentiality when the data is in storage but how the passwords are managed and enforced will either strengthen or weaken the effectiveness of that measure.

There are many risks associated with 'Confidentiality', for example: what is the risk and how will you protect personal information as it is being transported on the network; how will you protect personal information that is received or output in paper or other forms; how do you ensure that nobody can access the personal information from backup files; how do you ensure that personal information cannot be altered deliberately or accidentally?

When thinking about integrity the list of risks is equally as long. You must be able to ensure that you can prevent and detect alteration of data, even by a person with a password.

MM

All security must be "appropriate to the risk" so that will be up to you to decide depending on what controls you already have in place, the sensitivity of the data you hold and the threats to it.

I suspect client data is a pretty sensitive category so in my personal opinion, password protection will not be enough.

Firstly, you're going to have to assess what kind of client data you hold and whether you really need all of it. Minimising the amount of data you have should be a priority.

Password protection is a good start but you may want to consider further security measures. The GDPR recommends encrypting and pseudonymising data at rest - a process which renders personal data unreadable to anyone who gets unauthorised access.

Q What are the requirements to the organisation in case of a breach? I have heard that actions need to be taken within 72 hours. Is that correct?

A Ricoh Europe response:

MI

Data Controllers and Data Processors have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals (for example, a breach which, if unaddressed, would be likely to have a significant detrimental effect on individuals – such as resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage).

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine of up to 10 million euros or two per cent of your global turnover.

MM

In the case of your discovery of a breach - you will need to report it to the local regulator within 72 hours. If that breach results in theft or damage to personal data which could later harm its owner (through identity theft, for example) then you must report it to the data subject within 72 hours.

Even if you don't have to report - you must keep a record of those breaches in order to demonstrate compliance.

Aside from all of this, you'll have to set up appropriate security controls so that you can detect, find and respond to a breach in good time.

Q Will being GDPR ready mean you are covered for Network & Information Security (NIS) Directive regulations?

A Ricoh Europe response:

MI

There are many similarities between GDPR and NIS. NIS is the new EU legislation relating to the 2013 EU Cybersecurity Strategy. It requires operators of critical infrastructures and industry sectors to take steps to prevent and minimise the impact of incidents with a view of ensuring continuity of service.

The main differences between GDPR and NIS are the scope. GDPR applies to all organisations that process the personal information of EU data subjects. NIS applies to the operators of essential services defined by the EU member states and covers the entire information service.

Any organisation that has prepared for NIS compliance will be well positioned to be able to prove "adequate security" but will still need to ensure that they deliver privacy by design.

Q What data is subject to data portability?

A Ricoh Europe response:

MM

As is the remit of GDPR, personal data is subject to data portability. Article 20 of the GDPR sets this out: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided."

This means that people can ask for their data on request and it must be kept in a format where it can be moved from one system to another with ease. There are, however, some qualifications it makes. Data does not have to be portable if it is "necessary for the performance of a task carried out in the public interest" or if the transferral of that data would result in a risk to the rights and freedoms of other data subjects.

Q Who will be checking our organisation to confirm our compliance with GDPR? How long does this process take?

A Ricoh Europe response:

MI

Under GDPR the regulator can visit at any time. Organisations must be ready to provide records in order to prove their compliance.

Q Is there a defined retention period for which you are allowed to retain personal data, e.g. 5 years?

A Ricoh Europe response:

MI

Necessary retention periods are normally defined in the applicable national or industry specific regulations. For example, in the UK, finance information must be retained for the current tax year plus six years. The Data Controller should be aware of which regulations their organisation needs to comply with.

Q What if you needed to store the information for security reasons, for example, you didn't want to do business with this person in the future because of how they reacted previously. If the data is deleted we have no history.

A Ricoh Europe response:

MI

GDPR does not dictate what data is held. It requires you to define what personal information is held, the business reason for holding it, and that it is processed securely.

Q Would the GDPR include individuals' email addresses which are held under a Customer (Company) Account?

A Ricoh Europe response:

MM

I think this would go back to the ability to personally identify the data subject. Are these emails a "first name.last name@company.com" style of email address? If so, the answer would be yes. If they're something more obscure then perhaps not.

Q How do I log who had accessed documents on an MFP's Document Server?

A Ricoh Europe response:

MI

This depends on what hardware and software is in use. I'd suggest following up with your local Ricoh representative for further details.

Q How is GDPR enforced on non-EU organisations? Say, a Chinese company delivering to European consumers.

A Ricoh Europe response:

MM

GDPR will be enforced in the same way as it would on any organisation based within the EU, as long as the company processes the data of European citizens. This makes the GDPR almost a global piece of regulation considering that the EU is the largest economy in the world.

An organisation based outside of the EU will still have to show that they are looking after the personal data of European citizens, or face penalties. Companies that refuse those penalties will have a hard time continuing to do business in the world's largest market.

How aggressively the GDPR will be enforced on non-EU entities is yet to be seen. On paper however, they will be treated the same as any other organisation that handles the personal data of European citizens.

For further information on how Ricoh can help you improve your device, data and document security in preparation for GDPR, or to contact a Ricoh representative, visit us at ricoh-europe.com

RICOH
imagine. change.

www.ricoh-europe.com